MS221 EBD

The Open University

EXPLORING MATHEMATICS

Exercise Booklet D

Exercise Booklet

D

SUP 75905 5
1.2

Contents

Exercises for Chapter D1

Section 2

Exercise 2.1

Write down the real and imaginary parts of each of the following complex numbers.

(a) $\sqrt{3}+4i$ (b) 2.5 (c) $17i$

Exercise 2.2

Let $z=-3-4i$ and $w=6-2i$. Express each of the following complex numbers in the form $a+bi$.

(a) $z+w$ (b) $-w$ (c) $z-w$ (d) $-4z$

(e) zw (f) $\overline{z}$ (g) $z+\overline{z}$ (h) $z-\overline{z}$

(i) $z\overline{z}$ (j) $\overline{w}$ (k) $w\overline{w}$ (l) z^{-1}

(m) $\dfrac{w}{z}$ (n) $\dfrac{z}{w}$

Exercise 2.3

Let $z+\overline{z}=6$ and $z\overline{z}=25$. Find all possible solutions z.

Exercise 2.4

Calculate each of the following.

(a) $3+9i-(-2+10i)$

(b) $(1+2i)(-2+4i)(2-3i)$

(c) $2+3i(4+5i)+(2+6i)(2-3i)$

(d) $\dfrac{2+3i}{(-1-2i)^2}$

Exercise 2.5

Let $z=-2+3i$. Find the complex number w such that $wz=i$.

Section 3

Exercise 3.1

Find the modulus of each of the following complex numbers.

(a) $2+4i$ (b) 6 (c) $8i$

(d) $-2-7i$ (e) $3-5i$

Exercise 3.2

Let $z=\sqrt{3}-\sqrt{3}i$ and $w=-1-i$. Express each of the following complex numbers in the form $a+bi$.

(a) $z+\overline{w}$ (b) $z-\overline{w}$ (c) $|\overline{z}\,\overline{w}|$

(d) $|z|\overline{w}$ (e) $\overline{z}|w|$

Exercise 3.3

Find the Cartesian form of each of the following complex numbers given in polar form. (You should not need to use a calculator.)

(a) $\left\langle 2,\dfrac{\pi}{4}\right\rangle$ (b) $\left\langle 3,\dfrac{\pi}{2}\right\rangle$ (c) $\left\langle 4,\dfrac{3\pi}{4}\right\rangle$

(d) $\langle 3,\pi\rangle$ (e) $\left\langle 1,-\dfrac{\pi}{4}\right\rangle$

Exercise 3.4

Show the following points on an Argand diagram. Use the diagram to find a polar form for each of the complex numbers, giving the principal value of the argument in each case. (You should not need to use a calculator.)

(a) $5+5i$ (b) $-3+\sqrt{3}i$ (c) $-\sqrt{5}-\sqrt{5}i$

(d) $9\sqrt{3}-27i$

Exercise 3.5

Find polar forms for each of the complex numbers below, giving the principal value of the argument in each case. (You will need to use a calculator.)

(a) $-1-5i$ (b) $2-3i$

Exercise 3.6

Let $z=1+\sqrt{3}i$ and $w=\left\langle 3,\dfrac{\pi}{6}\right\rangle$.

(a) Express z in polar form, indicating all such representations.

(b) Express w in Cartesian form.

Exercise 3.7

Evaluate each of the following expressions. Give your answer in both Cartesian form and polar form, using the principal value of the argument. (You should not need to use a calculator.)

(a) $\left\langle 3,\dfrac{3\pi}{4}\right\rangle\times\left\langle 2,\dfrac{\pi}{2}\right\rangle$ (b) $\left\langle 1,\dfrac{\pi}{3}\right\rangle\times\left\langle 1,-\dfrac{\pi}{3}\right\rangle$

(c) $\left\langle 2,-\dfrac{3\pi}{4}\right\rangle^4$

Section 4

Exercise 4.1

Find polynomials with real coefficients whose roots are the following pairs of complex numbers.

(a) $1\pm 3i$ (b) $-2\pm i$

Exercise 4.2

Let a and b be real numbers, and let $z_0 = a + bi$. Show that

$$(z - z_0)(z - \overline{z}_0) = z^2 - 2az + a^2 + b^2.$$

(The solutions to Exercise 4.1 are both particular cases of this equation.)

Exercise 4.3

Find a polynomial with real coefficients, which has the four roots $2 \pm i$ and $-2 \pm i$.

Exercise 4.4

(a) Find all the fifth roots of -1024 in polar form.

(b) Use your answer to part (a) to factorise the polynomial $z^5 + 1024$ into polynomial factors with real coefficients, where the factors are either linear or quadratic.

Exercise 4.5

Find the four solutions of $z^4 = 2\sqrt{3} + 2i$ in polar form and then in Cartesian form.

Exercise 4.6

(a) Verify that $z = 1 + i$ is a solution of the equation $z^3 + 16z^2 - 34z + 36 = 0$.

(b) Write down a second solution of the equation.

(c) Find real numbers a and b such that

$$z^3 + 16z^2 - 34z + 36 = (z^2 - az + a)(z + b).$$

Section 5

Exercise 5.1

Write each of the complex numbers in Exercise 3.3 in exponential form.

Exercise 5.2

Use your answers to Exercise 3.6 to write $z = 1 + \sqrt{3}\,i$ and $w = \left\langle 3, \dfrac{\pi}{6} \right\rangle$ in Cartesian, polar and exponential forms.

Exercise 5.3

Express the following complex numbers in Cartesian form and in polar form.

(a) $z = e^{4-2i}$ (b) $w = \sqrt{10}e^{i\pi/4}$

Exercise 5.4

Use Euler's formula to verify the equation

$$e^{i\pi} + 1 = 0.$$

Exercises for Chapter D2

Section 1

Exercise 1.1

For each of the following integers a and n, find the quotient q and remainder r upon division of a by n.

(a) $a = 83$, $n = 7$

(b) $a = 509\,301$, $n = 9$

(c) $a = -26$, $n = 3$

(d) $a = -147$, $n = 5$

(e) $a = 212\,759$, $n = 6$

(f) $a = 10^7$, $n = 7$

Exercise 1.2

Decide which of the following congruences are true and which are false.

(a) $18 \equiv 12 \pmod 5$

(b) $26 \equiv 12 \pmod 7$

(c) $11 \equiv -5 \pmod 8$

(d) $5 \equiv 95 \pmod{20}$

(e) $95 \equiv 5 \pmod{20}$

(f) $-28 \equiv -16 \pmod 3$

Exercise 1.3

Use repeated multiplication to find the remainder when

(a) 4^{12} is divided by 9;

(b) 9^{112} is divided by 22;

(c) 3^{100} is divided by 16.

Exercise 1.4

Repeat Exercise 1.3 using repeated squaring.

Section 2

Exercise 2.1

Find the remainder when the sixteen-digit number 4321 2345 6789 8765 is divided by each of the following numbers.

(a) 3 (b) 9 (c) 11 (d) 2

(e) 4 (f) 8 (g) 6 (h) 12

(i) 7 (j) 13 (k) 5 (l) 10

Exercise 2.2

(a) A rule for finding the remainder r_{15} when a positive integer a is divided by 15, given the remainders r_3 and r_5 on division of a by 3 and 5, is

$$r_{15} \equiv 6r_5 - 5r_3 \pmod{15}.$$

Explain why this congruence is true.

(b) Use this rule to find the remainder when the integer in Exercise 2.1 is divided by 15.

Section 3

Exercise 3.1

Evaluate each of the following.

(a) $3 +_8 7$ (b) $2 +_7 5$ (c) $4 \times_{11} 9$

(d) $1 \times_4 2 \times_4 3$ (e) $8 \times_{10} 9$

(f) $1 +_9 (2 \times_9 8)$ (g) $(1 +_9 2)^{11} \times_9 8$

Exercise 3.2

(a) Give a condition for a number in $\mathbb{Z}_{60}$ to have a multiplicative inverse in $\mathbb{Z}_{60}$.

(b) Give an example of a number in $\mathbb{Z}_{60}$ that has a multiplicative inverse in $\mathbb{Z}_{60}$.

(c) Give an example of a number in $\mathbb{Z}_{60}$ that does not have a multiplicative inverse in $\mathbb{Z}_{60}$.

Exercise 3.3

Use Euclid's algorithm to find

(a) the multiplicative inverse of 5 in $\mathbb{Z}_7$;

(b) the multiplicative inverse of 12 in $\mathbb{Z}_{35}$;

(c) the multiplicative inverse of 23 in $\mathbb{Z}_{60}$.

Exercise 3.4

Use Fermat's Little Theorem to find the remainders when

(a) 7^{24} is divided by 11;

(b) 38^{51} is divided by 17;

(c) 14^{200} is divided by 5.

Section 4

In each of the following exercises, use the representation of the English alphabet given on page 39 of Chapter D2.

Exercise 4.1

A multiplicative cipher on $\mathbb{Z}_{26}$ is defined by the function

$$M_5(m) \equiv 5 \times_{26} m.$$

(a) Determine the multiplicative inverse of 5 in $\mathbb{Z}_{26}$.

(b) A message is enciphered using M_5 to give the ciphertext

$$\langle 3, 25, 25, 2, 17, 13, 19, 8, 19, 18, 9 \rangle.$$

What was the message?

Exercise 4.2

An exponential cipher is defined on $\mathbb{Z}_{31}$ by the function

$$E_7(m) \equiv m^7 \pmod{31}.$$

(a) Determine the multiplicative inverse of 7 in $\mathbb{Z}_{30}$.

(b) A message was enciphered using E_7 to give the ciphertext $\langle 2, 10 \rangle$. What was the message?

Exercise 4.3

An RSA cipher is defined on $\mathbb{Z}_{51}$ by the function

$$R_{25}(m) \equiv m^{25} \pmod{51}.$$

(a) Determine the multiplicative inverse of 25 in $\mathbb{Z}_{32}$.

(b) A message was enciphered by R_{25} to give the ciphertext $\langle 8, 29, 39, 16 \rangle$. What was the message?

Exercises for Chapter D3

Section 1

Exercise 1.1

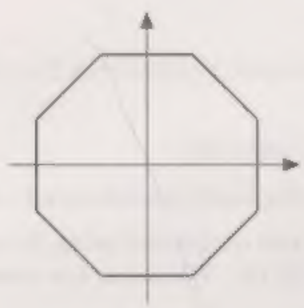
Evaluate the following.

(a) $r_\pi(1,0)$ (b) $q_0(2,0)$

(c) $q_{\pi/4}(1,2)$ (d) $r_{3\pi/2}(2,3)$

Exercise 1.2

Using the r_θ, q_ϕ notation, write down $S(\text{OCT})$, the set of symmetries of the regular octagon in standard position.



Exercise 1.3

Use Table 1.3 to find the following composite symmetries.

(a) $r_{\pi/3} \circ r_{5\pi/3}$

(b) $q_{\pi/2} \circ q_{\pi/4}$

(c) $r_\pi \circ q_{\pi/2}$

Exercise 1.4

Construct a Cayley table for

$$S(\text{HEX}) = \{e, r_{\pi/3}, r_{2\pi/3}, r_\pi, r_{4\pi/3}, r_{5\pi/3}, q_0, q_{\pi/6}, q_{\pi/3}, q_{\pi/2}, q_{2\pi/3}, q_{5\pi/6}\}.$$

(This exercise is intended to provide plenty of practice in composing symmetries.)

Section 2

Exercise 2.1

Use your Cayley table from Exercise 1.4 to determine the inverse of each element of $S(\text{HEX})$.

Exercise 2.2

Use your Cayley table from Exercise 1.4 to check that the following are equal:

$$q_{\pi/3} \circ \left(r_{2\pi/3} \circ q_{5\pi/6}\right) \text{ and } \left(q_{\pi/3} \circ r_{2\pi/3}\right) \circ q_{5\pi/6}.$$

Exercise 2.3

(a) Prove that $(\mathbb{Q}, \times)$ is not a group; that is, show that the set of rational numbers under multiplication does not form a group.

(b) Is $(\mathbb{Q}^*, \times)$ a group?

Exercise 2.4

Construct Cayley tables for each of the following sets and operations, and verify that each forms an Abelian group.

(a) $\{1,3,5,7\}$ under $\times_8$

(b) $\{1,3,7,9\}$ under $\times_{10}$

(c) $\{1,5,7,11\}$ under $\times_{12}$

(d) $\{2,4\}$ under $\times_6$

(e) $\{0,2,4,6,8\}$ under $+_{10}$

Exercise 2.5

Let

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{A} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{C} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(a) Show that $M = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ forms a group under matrix multiplication.

(b) Find a symmetry group corresponding to $(M, \times)$.

Exercise 2.6

Show that $(3\mathbb{Z}, +)$ is a group, where

$3\mathbb{Z} = \{3k : k \text{ is an integer}\}$.

Exercise 2.7

Let $G = \{5^k : k \text{ is an integer}\}$. Show that $(G, \times)$ is a group.

Exercise 2.8

Given that each of the following Cayley tables represents a group, fill in the missing elements.

(a)

$*$	e	x	y
e	e	x	y
x	x		
y	y		

(b)

$*$	w	x	y	z
w	z			w
x		z		
y	x			y
z	w	x	y	

Exercise 2.9

Let $(G, *)$ be a group with g and h elements of G. Show that, for all natural numbers n,

$$(g * h * g^{-1})^n = g * h^n * g^{-1}.$$

Section 3

Exercise 3.1

Find a plane set which has a symmetry group isomorphic to $(\mathbb{Z}_4, +_4)$.

Exercise 3.2

Show that the Cayley table of the group in Exercise 2.8(b) can be rearranged so that its pattern is the same as that of $(S(\square), \circ)$, given in Activity 1.7(c) of the main text.

Exercise 3.3

One of the groups in Exercise 2.4 is isomorphic to the group of rotations of a square. Identify it, giving reasons.

Exercise 3.4

A Cayley table for a group is given below:

$\circ$	a	b	c	d	e	x	y	z
a	y	d	b	z	x	a	e	c
b	c	y	e	a	d	b	z	x
c	z	a	y	x	b	c	d	e
d	b	e	x	y	z	d	c	a
e	x	c	z	b	y	e	a	d
x	a	b	c	d	e	x	y	z
y	e	z	d	c	a	y	x	b
z	d	x	a	e	c	z	b	y

(a) What is the identity element of the group?

(b) State the inverse of each element of the group.

(c) To which group, mentioned in Chapter D3, is this group isomorphic?

Exercise 3.5

Show that $(\mathbb{Z}_6, +_6)$ is not isomorphic to $(S(\Delta), \circ)$.

Exercises for Chapter D4

Section 1

Exercise 1.1

Consider the statements below. In each case, either provide a proof to show that the statement is true or give a counter-example to show that the statement is false.

(a) There exists a real number, x, such that $x^2 - 2x = 15$.

(b) The function $f(x) = 3x + 2$ is increasing on $\mathbb{R}$.

(c) For any 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$, if $\mathbf{AB} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, then $\mathbf{A} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ or $\mathbf{B} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(d) For all natural numbers n, if 2 divides n, then 4 divides n^2.

(e) For all natural numbers n, the expression $n^2 + n + 41$ is prime.

Exercise 1.2

Where is the reasoning false in the following argument?

Since $2 > 1$, we have

$$2\ln(0.5) > \ln(0.5).$$

Thus

$$\ln(0.5^2) > \ln(0.5),$$

so

$$\ln(0.25) > \ln(0.5)$$

and hence $0.25 > 0.5$.

Exercise 1.3

Use proof by exhaustion to show that the equation $x^3 = 4$ has exactly one solution in $\mathbb{Z}_5$.

Exercise 1.4

Prove that for all integers n, if 3 divides n, then 3 divides $5n - 6$.

Exercise 1.5

Prove that the product of any three consecutive positive integers is divisible by 6.

Exercise 1.6

Use proof by exhaustion to show that for any integer n, if n is not divisible by 3, then n^2 has a remainder of 1 on division by 3.

(*Hint*: If n is not divisible by 3, then n must be congruent modulo 3 to either 1 or 2.)

Exercise 1.7

Show that the function $f(x) = 4x + 5$ ($x \in \mathbb{R}$) is one-one.

Exercise 1.8

Show that the set

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \text{ real numbers with } ab = 1 \right\}$$

is closed under matrix multiplication.

Exercise 1.9

(a) Show that

(i) the sum of two odd numbers is even;

(ii) the sum of two even numbers is even;

(iii) the sum of an odd number and an even number is odd.

(b) Show that

(i) the square of an odd number is odd;

(ii) the square of an even number is even.

Exercise 1.10

Prove, by contradiction, that if the integer n^2 is divisible by 3, then the integer n is divisible by 3.

Section 2

Exercise 2.1

The variable propositions $a(n)$, $b(n)$, $c(n)$ and $d(n)$, where n is a natural number, have the meanings given below:

$a(n)$ means: n is divisible by 2;
$b(n)$ means: n is divisible by 4;
$c(n)$ means: n is divisible by 5;
$d(n)$ means: n is divisible by 40.

(a) For each of $a(n)$, $b(n)$, $c(n)$ and $d(n)$, say whether it is necessary but not sufficient, sufficient but not necessary, necessary and sufficient or neither necessary nor sufficient, in order that n be divisible by 20.

(b) Give a condition that is necessary and sufficient for n to be divisible by 10, using a combination of the propositions above.

(c) Write down in words the proposition

$$(a(n) \wedge c(n)) \Rightarrow d(n).$$

(d) Write down, in symbols and in words, the converse of the proposition in part (c).

(e) Write down a counter-example to show that the proposition in part (c) is false.

Exercise 2.2

Consider the proposition

if $\theta = \pi$, then $\sin\theta = 0$.

(a) Write down the converse of the above proposition.

(b) Is the original proposition true?

(c) Is the converse of the original proposition true?

Justify your answers to parts (b) and (c).

Exercise 2.3

Below are four attempts at deductions. Which of these deductions are valid? Where possible, define propositions p and q so that the form of the deduction is Modus Ponens.

(a) We know that:

on hot days my plants must be watered;
it is a hot day.

We conclude that:

my plants must be watered.

(b) We know that:

Greg goes to the mountains on Saturdays;
Greg has gone to the mountains.

We conclude that:

it is a Saturday.

(c) We know that:

all elephants have trunks;
Zeya does not have a trunk.

We conclude that:

Zeya is not an elephant.

(d) We know that:

if $(H, *)$ and $(G, \circ)$ are finite isomorphic groups, then $|G| = |H|$;
$(H, *)$ and $(G, \circ)$ are finite non-isomorphic groups.

We conclude that:

$|H| \neq |G|$.

Section 3

Exercise 3.1

Suppose that $x \equiv y \pmod{m}$ for integers x, y and $m > 0$.

Prove, by mathematical induction, that for every natural number n we have $x^n \equiv y^n \pmod{m}$.

Exercise 3.2

Let $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$.

(a) Find $\mathbf{A}^2$, $\mathbf{A}^3$, $\mathbf{A}^4$ and $\mathbf{A}^5$, and conjecture a formula for $\mathbf{A}^n$, for $n = 1, 2, \ldots$.

(b) Prove your conjecture by mathematical induction.

Exercise 3.3

Prove by mathematical induction that

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}, \quad \text{for } n = 1, 2, 3, \ldots.$$

Exercise 3.4

The sequence of real numbers, $u_1, u_2, u_3, \ldots$, is defined as

$$u_1 = 3.5, \quad u_{n+1} = 4 - \frac{5}{u_n + 2} \quad (n = 1, 2, \ldots).$$

Show that $u_n > 3$ for all $n \in \mathbb{N}$.

Exercise 3.5

Prove by mathematical induction that the following identity is true:

$$\sum_{r=1}^{n} \frac{r}{2^r} = 2 - \frac{n+2}{2^n}, \quad \text{for } n = 1, 2, 3 \ldots.$$

Exercise 3.6

Consider the function $f(x) = x^2 e^x$. Prove, using mathematical induction, that $f^{(n)}$, the nth derivative of f, has the rule

$$f^{(n)}(x) = x^2 e^x + 2nxe^x + n(n-1)e^x, \quad \text{for } n \geq 1.$$

Exercise 3.7

Show, using the generalised form of mathematical induction, that

$$n! > 2^n, \quad \text{for } n \geq 4.$$

Solutions for Chapter D1

Solution 2.1

(a) $\operatorname{Re}(\sqrt{3}+4i)=\sqrt{3}$, $\quad \operatorname{Im}(\sqrt{3}+4i)=4$

(b) $\operatorname{Re}(2.5)=2.5$, $\quad \operatorname{Im}(2.5)=0$

(c) $\operatorname{Re}(17i)=0$, $\quad \operatorname{Im}(17i)=17$

(Note that the imaginary part of a complex number is always a real number.)

Solution 2.2

(a) $3-6i$ (b) $-6+2i$ (c) $-9-2i$

(d) $12+16i$ (e) $-26-18i$ (f) $-3+4i$

(g) -6 (h) $-8i$ (i) 25

(j) $6+2i$ (k) 40

(l) $$\begin{aligned} z^{-1} &= \frac{1}{-3-4i} = \frac{-3+4i}{(-3-4i)(-3+4i)} \\ &= \frac{-3+4i}{25} = -\tfrac{3}{25}+\tfrac{4}{25}i \end{aligned}$$

(m) $$\begin{aligned} \frac{w}{z} &= \frac{6-2i}{-3-4i} = \frac{(6-2i)(-3+4i)}{(-3-4i)(-3+4i)} \\ &= \frac{-10+30i}{25} = -\tfrac{2}{5}+\tfrac{6}{5}i \end{aligned}$$

(n) $$\begin{aligned} \frac{z}{w} &= \frac{-3-4i}{6-2i} = \frac{(-3-4i)(6+2i)}{(6-2i)(6+2i)} \\ &= \frac{-10-30i}{40} = -\tfrac{1}{4}-\tfrac{3}{4}i \end{aligned}$$

Solution 2.3

Let $z=x+yi$. Then

$$z+\overline{z}=x+yi+x-yi=2x=6,$$

so $x=3$. Also,

$$z\overline{z}=(x+yi)(x-yi)=x^2+y^2=25,$$

so

$$y^2=25-x^2=25-9=16.$$

Hence $y=\pm 4$, so

$$z=3+4i \quad \text{or} \quad z=3-4i.$$

Solution 2.4

(a) $5-i$

(b) $-20+30i$

(c) $9+18i$

(d) $$\begin{aligned} \frac{2+3i}{(-1-2i)^2} &= \frac{2+3i}{-3+4i} \\ &= \frac{(2+3i)(-3-4i)}{(-3+4i)(-3-4i)} \\ &= \frac{6-17i}{25} = \tfrac{6}{25}-\tfrac{17}{25}i \end{aligned}$$

Solution 2.5

We have

$$\begin{aligned} w &= \frac{i}{z} = \frac{i}{-2+3i} \\ &= \frac{i(-2-3i)}{(-2+3i)(-2-3i)} \\ &= \frac{3-2i}{4+9} = \tfrac{3}{13}-\tfrac{2}{13}i. \end{aligned}$$

Solution 3.1

(a) $|2+4i|=\sqrt{2^2+4^2}=\sqrt{20}=2\sqrt{5}$

(b) $|6|=\sqrt{6^2}=6$

(c) $|8i|=\sqrt{8^2}=8$

(d) $|-2-7i|=\sqrt{(-2)^2+(-7)^2}=\sqrt{53}$

(e) $|3-5i|=\sqrt{3^2+(-5)^2}=\sqrt{34}$

Solution 3.2

(a) $\sqrt{3}-1+(-\sqrt{3}+1)i$

(b) $\sqrt{3}+1-(\sqrt{3}+1)i$

(c) $|-2\sqrt{3}|=2\sqrt{3}$

(d) $\sqrt{6}(-1+i)=-\sqrt{6}+\sqrt{6}\,i$

(e) $(\sqrt{3}+\sqrt{3}\,i)\times\sqrt{2}=\sqrt{6}+\sqrt{6}\,i$

Solution 3.3

(a) $$\begin{aligned} \left\langle 2,\frac{\pi}{4}\right\rangle &= 2\cos\left(\frac{\pi}{4}\right)+2i\sin\left(\frac{\pi}{4}\right) \\ &= \frac{2}{\sqrt{2}}+\frac{2}{\sqrt{2}}i \\ &= \sqrt{2}+\sqrt{2}\,i \end{aligned}$$

(b) $$\begin{aligned} \left\langle 3,\frac{\pi}{2}\right\rangle &= 3\cos\left(\frac{\pi}{2}\right)+3i\sin\left(\frac{\pi}{2}\right) \\ &= 3i \end{aligned}$$

(c) $$\begin{aligned} \left\langle 4,\frac{3\pi}{4}\right\rangle &= 4\cos\left(\frac{3\pi}{4}\right)+4i\sin\left(\frac{3\pi}{4}\right) \\ &= -\frac{4}{\sqrt{2}}+\frac{4}{\sqrt{2}}i \\ &= -2\sqrt{2}+2\sqrt{2}\,i \end{aligned}$$

(d) $$\begin{aligned} \langle 3,\pi\rangle &= 3\cos(\pi)+3i\sin(\pi) \\ &= -3 \end{aligned}$$

(e) $$\begin{aligned} \left\langle 1,-\frac{\pi}{4}\right\rangle &= \cos\left(-\frac{\pi}{4}\right)+i\sin\left(-\frac{\pi}{4}\right) \\ &= \frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i \end{aligned}$$

Solution 3.4

Remark: There are other valid methods of arriving at the solution for parts (a)–(e). For example, you may prefer to find $\cos\theta$ and $\sin\theta$ in each case. Note that all angles are given in radians.

(a)

We have

$$r = \sqrt{5^2 + 5^2} = \sqrt{50} = 5\sqrt{2}.$$

This complex number lies in the first quadrant of the Argand diagram and the angle θ satisfies

$$\tan\theta = \frac{5}{5} = 1 \quad \text{so} \quad \theta = \arctan(1) = \frac{\pi}{4}.$$

Thus the required polar form is $\left\langle 5\sqrt{2}, \frac{\pi}{4}\right\rangle$.

(b)

We have

$$r = \sqrt{(-3)^2 + (\sqrt{3})^2} = \sqrt{12} = 2\sqrt{3}.$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{\sqrt{3}}{3} \quad \text{so} \quad \alpha = \frac{\pi}{6}.$$

Hence

$$\theta = \pi - \frac{\pi}{6} = \frac{5\pi}{6}.$$

This is the principal value of the argument, as $-\pi < \theta \leq \pi$.

Thus the required polar form is $\left\langle 2\sqrt{3}, \frac{5\pi}{6}\right\rangle$.

(c)

We have

$$r = \sqrt{(-\sqrt{5})^2 + (-\sqrt{5})^2} = \sqrt{10}$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{\sqrt{5}}{\sqrt{5}} = 1 \quad \text{so} \quad \alpha = \frac{\pi}{4}.$$

Hence

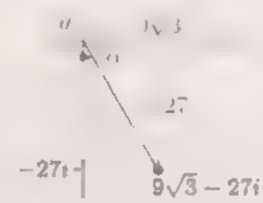
$$\theta = \pi + \frac{\pi}{4} = \frac{5\pi}{4}.$$

This is not the principal value of the argument, as it does not lie within the range $-\pi < \theta \leq \pi$. The principal value of the argument is

$$\frac{5\pi}{4} - 2\pi = -\frac{3\pi}{4}.$$

Thus the required polar form is $\left\langle \sqrt{10}, -\frac{3\pi}{4}\right\rangle$.

(d)



We have

$$r = \sqrt{(9\sqrt{3})^2 + (-27)^2} = \sqrt{972} = 18\sqrt{3}.$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{27}{9\sqrt{3}} = \sqrt{3} \quad \text{so} \quad \alpha = \frac{\pi}{3}.$$

Hence

$$\theta = 2\pi - \frac{\pi}{3} = \frac{5\pi}{3}.$$

The principal value of the argument is

$$\frac{5\pi}{3} - 2\pi = -\frac{\pi}{3}.$$

Thus the required polar form is $\left\langle 18\sqrt{3}, -\frac{\pi}{3}\right\rangle$.

Solution 3.5

(a)

We have

$$r = \sqrt{(-1)^2 + (-5)^2} = \sqrt{26} = 5.099 \text{ (to 3 d.p.)}.$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{5}{1} \quad \text{so} \quad \alpha = \arctan(5) = 1.3734\ldots.$$

Hence

$$\theta = \pi + \arctan(5) = 4.5149\ldots.$$

The principal value of the argument is

$$\theta - 2\pi = -1.768 \text{ (to 3 d.p.)}.$$

Thus the required polar form is $\langle 5.099, -1.768\rangle$ to three decimal places.

(b)

We have

$$r = \sqrt{2^2 + (-3)^2} = \sqrt{13} = 3.606 \text{ (to 3 d.p.)}.$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{3}{2} \quad \text{so} \quad \alpha = \arctan\left(\frac{3}{2}\right) = 0.9827\ldots.$$

Hence the principal value of the argument is -0.983 (to 3 d.p.). Thus the required polar form is $\langle 3.606, -0.983\rangle$ to three decimal places.

Solution 3.6

(a)

We have

$$r = \sqrt{1^2 + (\sqrt{3})^2} = 2.$$

The angle α in the diagram satisfies

$$\tan\alpha = \frac{\sqrt{3}}{1} \quad \text{so} \quad \alpha = \frac{\pi}{3}.$$

This is the principal value of the argument, so a polar form is $\left\langle 2, \frac{\pi}{3}\right\rangle$. Other representations in polar form can be found by adding integer multiples of 2π to the principal argument. In general, $1 + \sqrt{3}i$ is represented in polar form as $\left\langle 2, \frac{\pi}{3} + 2n\pi\right\rangle$ where n is any integer.

(b) We have

$$w = \left\langle 3, \frac{\pi}{6}\right\rangle = 3\cos\left(\frac{\pi}{6}\right) + 3i\sin\left(\frac{\pi}{6}\right)$$
$$= \frac{3\sqrt{3}}{2} + \frac{3}{2}i.$$

Solution 3.7

(a) Polar form:

$$\left\langle 3, \frac{3\pi}{4}\right\rangle \times \left\langle 2, \frac{\pi}{2}\right\rangle = \left\langle 3 \times 2, \frac{3\pi}{4} + \frac{\pi}{2}\right\rangle$$
$$= \left\langle 6, \frac{5\pi}{4}\right\rangle = \left\langle 6, -\frac{3\pi}{4}\right\rangle$$

Cartesian form:

$$\left\langle 6, -\frac{3\pi}{4}\right\rangle = 6\cos\left(-\frac{3\pi}{4}\right) + 6i\sin\left(-\frac{3\pi}{4}\right)$$
$$= -\frac{6}{\sqrt{2}} - \frac{6}{\sqrt{2}}i = -3\sqrt{2} - 3\sqrt{2}i.$$

(b) Polar form:

$$\left\langle 1, \frac{\pi}{3}\right\rangle \times \left\langle 1, -\frac{\pi}{3}\right\rangle = \langle 1, 0\rangle.$$

Cartesian form:

$$\langle 1, 0\rangle = \cos 0 + i\sin 0 = 1.$$

(c) Polar form:

$$\left\langle 2, -\frac{3\pi}{4}\right\rangle^4 = \left\langle 2^4, 4 \times \left(-\frac{3\pi}{4}\right)\right\rangle$$
$$= \langle 16, -3\pi\rangle = \langle 16, \pi\rangle.$$

Cartesian form:

$$\langle 16, \pi\rangle = 16\cos\pi + i\sin\pi = -16.$$

Solution 4.1

(a) $\big(x - (1 + 3i)\big)\big(x - (1 - 3i)\big) = x^2 - 2x + 10$

(b) $\big(x - (-2 + i)\big)\big(x - (-2 - i)\big) = x^2 + 4x + 5$

Solution 4.2

We have

$$\begin{aligned}(z - z_0)(z - \overline{z}_0) &= z^2 - (z_0 + \overline{z}_0)z + z_0\overline{z}_0 \\ &= z^2 - (a + bi + a - bi)z \\ &\quad + (a + bi)(a - bi) \\ &= z^2 - 2az + a^2 + b^2,\end{aligned}$$

as required.

Solution 4.3

A suitable polynomial is

$$(x - (2 + i))(x - (2 - i))(x - (-2 + i))(x - (-2 - i)).$$

By Exercise 4.2, this polynomial is of the form

$$(x^2 - 4x + 5)(x^2 + 4x + 5) = x^4 - 6x^2 + 25.$$

Solution 4.4

(a) Let $w = -1024$. First of all, we express w in polar form:

We have $|w| = 1024$ and $\arg w = \pi$, so in polar form $w = \langle 1024, \pi \rangle$.

The fifth roots of -1024 are solutions of $z^5 = -1024$.

Now if $z = \langle r, \theta \rangle$, then

$$z^5 = \langle r, \theta \rangle^5 = \langle r^5, 5\theta \rangle = \langle 1024, \pi \rangle.$$

Thus $r^5 = 1024$, so

$$r = 1024^{1/5} = 4.$$

Also $5\theta = \pi + 2\pi m$, so

$$\theta = \frac{\pi + 2\pi m}{5}, \text{ where } m = 0, 1, 2, 3, 4.$$

Thus the fifth roots are

[illegible]

(b) First note that

$$z_0 = 4(\cos(\pi/5) + i\sin(\pi/5)),$$
$$z_1 = 4(\cos(3\pi/5) + i\sin(3\pi/5)),$$
$$z_2 = 4(\cos\pi + i\sin\pi) = -4.$$

By Exercise 4.2, the conjugate pairs z_0, z_4 and z_1, z_3 give rise to quadratic factors

$$(z - z_0)(z - z_4) = z^2 - 8\cos\left(\frac{\pi}{5}\right) z + 16,$$
$$(z - z_1)(z - z_3) = z^2 - 8\cos\left(\frac{3\pi}{5}\right) z + 16,$$

and z_2 gives the linear factor

$$(z - z_2) = (z - (-4)) = (z + 4).$$

Putting these together, we obtain

$$z^5 + 1024 = (z + 4)\left(z^2 - 8\cos\left(\frac{\pi}{5}\right) z + 16\right)$$
$$\times \left(z^2 - 8\cos\left(\frac{3\pi}{5}\right) z + 16\right).$$

Solution 4.5

First we express $w = 2\sqrt{3} + 2i$ in polar form. We have

$$r = \sqrt{(2\sqrt{3})^2 + 2^2} = 4,$$

and the principal argument α satisfies

$$\tan\alpha = \frac{2}{2\sqrt{3}} \quad \text{so} \quad \alpha = \arctan\left(\frac{1}{\sqrt{3}}\right) = \frac{\pi}{6}.$$

Thus $w = \left\langle 4, \frac{\pi}{6} \right\rangle$.

The fourth roots of w are found by solving

$$\langle r, \theta \rangle^4 = \langle r^4, 4\theta \rangle = \left\langle 4, \frac{\pi}{6} \right\rangle.$$

This gives $r^4 = 4$, so

$$r = \sqrt{2},$$

and $4\theta = \pi/6 + 2\pi m$, so

$$\theta = \frac{\pi/6 + 2\pi m}{4}, \text{ where } m = 0, 1, 2, 3.$$

Thus the four fourth roots are

$$z_0 = \left\langle \sqrt{2}, \frac{\pi}{24} \right\rangle,$$
$$z_1 = \left\langle \sqrt{2}, \frac{13\pi}{24} \right\rangle,$$
$$z_2 = \left\langle \sqrt{2}, \frac{25\pi}{24} \right\rangle = \left\langle \sqrt{2}, -\frac{23\pi}{24} \right\rangle,$$
$$z_3 = \left\langle \sqrt{2}, \frac{37\pi}{24} \right\rangle = \left\langle \sqrt{2}, -\frac{11\pi}{24} \right\rangle$$

These roots can be written in Cartesian form, correct to three decimal places, as follows.

$$\begin{aligned} z_0 &= \sqrt{2}\left(\cos\left(\frac{\pi}{24}\right) + i\sin\left(\frac{\pi}{24}\right)\right) \\ &= 1.402 + 0.185i \\ z_1 &= \sqrt{2}\left(\cos\left(\frac{13\pi}{24}\right) + i\sin\left(\frac{13\pi}{24}\right)\right) \\ &= -0.185 + 1.402i \\ z_2 &= \sqrt{2}\left(\cos\left(\frac{25\pi}{24}\right) + i\sin\left(\frac{25\pi}{24}\right)\right) \\ &= -1.402 - 0.185i \\ z_3 &= \sqrt{2}\left(\cos\left(\frac{37\pi}{24}\right) + i\sin\left(\frac{37\pi}{24}\right)\right) \\ &= 0.185 - 1.402i \end{aligned}$$

Solution 4.6

(a) We have $(1+i)^2 = 1 + 2i - 1 = 2i$, so

$$(1+i)^3 = 2i(1+i) = -2 + 2i.$$

Thus

$$\begin{aligned} &(1+i)^3 + 16(1+i)^2 - 34(1+i) + 36 \\ &= -2 + 2i + 32i - 34 - 34i + 36 \\ &= 0. \end{aligned}$$

So $z = 1 + i$ is indeed a solution of $z^3 + 16z^2 - 34z + 36 = 0$.

(b) Since the equation has real coefficients, if $z = 1 + i$ is a solution then $\overline{z} = 1 - i$ is also a solution.

(c) By parts (a) and (b), the product

$$(z - (1+i))(z - (1-i)) = z^2 - 2z + 2$$

is a factor of the equation. Thus $a = 2$. Now

$$\begin{aligned} &z^3 + 16z^2 - 34z + 36 \\ &\qquad = (z^2 - 2z + 2)(z + b) \\ &\qquad = z^3 - 2z^2 + 2z + bz^2 - 2bz + 2b \\ &\qquad = z^3 + (b-2)z^2 + (2-2b)z + 2b. \end{aligned}$$

Comparing coefficients, we have

$$b - 2 = 16 \quad \text{so} \quad b = 18$$

which also satisfies $2 - 2b = -34$ and $2b = 36$. Hence

$$z^3 + 16z^2 - 34z + 36 = (z^2 - 2z + 2)(z + 18).$$

Solution 5.1

Notice that if the polar form is known then the exponential form can be written down immediately.

(a) $\left\langle 2, \frac{\pi}{4} \right\rangle = 2e^{i\pi/4}$

(b) $\left\langle 3, \frac{\pi}{2} \right\rangle = 3e^{i\pi/2}$

(c) $\left\langle 4, \frac{3\pi}{4} \right\rangle = 4e^{3i\pi/4}$

(d) $\langle 3, \pi \rangle = 3e^{i\pi}$

(e) $\left\langle 1, -\frac{\pi}{4} \right\rangle = e^{-i\pi/4}$

Solution 5.2

Using Solution 3.6(a), we obtain

$$z = 1 + \sqrt{3}\,i = \left\langle 2, \frac{\pi}{3} \right\rangle = 2e^{i\pi/3}.$$

(More generally, as seen in Solution 3.6(a), we have $z = \left\langle 2, \frac{\pi}{3} + 2m\pi \right\rangle$. The general exponential form is thus

$$z = 2e^{i(\pi/3 + 2m\pi)}, \quad \text{for any integer } m.)$$

Using Solution 3.6(b), we obtain

$$w = \frac{3\sqrt{3}}{2} + \frac{3}{2}i = \left\langle 3, \frac{\pi}{6} \right\rangle = 3e^{i\pi/6}.$$

Solution 5.3

(a) In Cartesian form,

$$\begin{aligned} z = e^{4-2i} &= e^4 \times e^{-2i} \\ &= e^4(\cos(-2) + i\sin(-2)) \\ &= -22.721 - 49.646i \text{ (to 3 d.p.)}. \end{aligned}$$

In polar form, $z = \langle e^4, -2 \rangle$.

(In general,

$$e^{a+bi} = \langle e^a, b \rangle = e^a(\cos b + i\sin b).)$$

(b) In Cartesian form,

$$\begin{aligned} w = \sqrt{10}e^{i\pi/4} &= \sqrt{10}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right) \\ &= \sqrt{10}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) \\ &= \sqrt{5} + \sqrt{5}i. \end{aligned}$$

In polar form,

$$w = \sqrt{10}e^{i\pi/4} = \left\langle \sqrt{10}, \frac{\pi}{4} \right\rangle.$$

Solution 5.4

Substituting $\theta = \pi$ into Euler's formula gives

$$e^{i\pi} = \cos\pi + i\sin\pi = -1.$$

Hence

$$e^{i\pi} + 1 = 0.$$

This equation appears in Euler's treatise *Introductio in analysin infinitorum* (Introduction to infinite analysis), published in 1748. It is one of the most remarkable identities in mathematics, as it includes the five fundamental constants, 0, 1, e, π and i, in one simple equation.

Solutions for Chapter D2

Solution 1.1

There is no need to use $q = \text{floor}(a/n)$, if you can 'see' how the division of a by n works out.

(a) We have $83 = 11 \times 7 + 6$, so $q = 11$ and $r = 6$.

(b) We have

$$q = \text{floor}\left(\frac{509\,301}{9}\right) = \text{floor}\,(56\,589) = 56\,589,$$

so $r = 0$.

(c) We have

$$q = \text{floor}\left(-\frac{26}{3}\right) = \text{floor}\,(-8.6\ldots) = -9,$$

so $r = -26 - (-9) \times 3 = 1$.

(d) We have

$$q = \text{floor}\left(-\frac{147}{5}\right) = \text{floor}\,(-29.4) = -30,$$

so $r = -147 - (-30) \times 5 = 3$.

(e) We have

$$q = \text{floor}\left(\frac{212\,759}{6}\right) = \text{floor}\,(35\,459.8\ldots)$$
$$= 35\,459,$$

so $r = 212\,759 - 35\,459 \times 6 = 5$.

(f) We have

$$q = \text{floor}\left(\frac{10^7}{7}\right) = \text{floor}\,(1\,428\,571.4\ldots)$$
$$= 1\,428\,571,$$

so $r = 10^7 - 1\,428\,571 \times 7 = 3$.

Solution 1.2

To show that $a \equiv b \pmod{n}$, you can either show that a and b have the same remainder when divided by n or show that $a - b$ is a multiple of n.

(a) False: $18 - 12 = 6$, which is not a multiple of 5.

(b) True: $26 - 12 = 14$, which is a multiple of 7.

(c) True: $11 - (-5) = 16$, which is a multiple of 8.

(d) False: $5 \div 20 = 0$ remainder 5; $95 \div 20 = 4$ remainder 15, and $5 \neq 15$

(e) False: Since (d) is false, (e) is also false.

(f) True: $-28 - (-16) = -12$, which is a multiple of 3.

Solution 1.3

(a) Repeated multiplication by 4 gives the following table

4^k	4^0	4^1	4^2	4^3
$4^k \pmod{9}$	1	4	7	1

So $4^k \equiv 1 \pmod{9}$, when k is a multiple of 3.

Thus $4^{12} \equiv 1 \pmod{9}$, since 12 is a multiple of 3. Hence the remainder is 1.

(b) Repeated multiplication by 9 gives the following table

9^k	9^0	9^1	9^2	9^3	9^4	9^5
$9^k \pmod{22}$	1	9	15	3	5	1

So $9^k \equiv 1 \pmod{22}$, when k is a multiple of 5.

Thus $9^{110} \equiv 1 \pmod{22}$ so

$$9^{112} \equiv 9^{110} \times 9^2 \equiv 9^2 \equiv 15 \pmod{22}$$

Hence the remainder is 15.

(c) Repeated multiplication by 3 gives the following table

3^k	3^0	3^1	3^2	3^3	3^4
$3^k \pmod{16}$	1	3	9	11	1

So $3^k \equiv 1 \pmod{16}$, when k is a multiple of 4.

Thus $3^{100} \equiv 1 \pmod{16}$, since 100 is a multiple of 4. Hence the remainder is 1.

Solution 1.4

(a) Repeated squaring gives

4^{2^n}	4^1	4^2	4^4	4^8
$4^{2^n} \pmod 9$	4	7	4	7

so

$$4^{12} \equiv 4^8 \times 4^4 \equiv 7 \times 4 \equiv 1 \pmod 9.$$

As expected, the remainder is 1.

(b) Repeated squaring gives

9^{2^n}	9^1	9^2	9^4	9^8	9^{16}	9^{32}	9^{64}
$9^{2^n} \pmod{22}$	9	15	5	3	9	15	5

so

$$9^{112} \equiv 9^{16} \times 9^{32} \times 9^{64} \equiv 9 \times 15 \times 5 \equiv 15 \pmod{22}.$$

As expected, the remainder is 15.

(c) Repeated squaring gives

3^{2^n}	3^1	3^2	3^4	3^8	3^{16}	3^{32}	3^{64}
$3^{2^n} \pmod{16}$	3	9	1	1	1	1	1

so

$$3^{100} \equiv 3^4 \times 3^{32} \times 3^{64} \equiv 1 \times 1 \times 1 \equiv 1 \pmod{16}.$$

As expected, the remainder is 1.

Solution 2.1

(a) The digit sum is $80 = 26 \times 3 + 2$, so $r_3 = 2$.

(b) The digit sum is $80 = 8 \times 9 + 8$, so $r_9 = 8$.

(c) The alternating digit sum is

$$\begin{aligned}&5 - 6 + 7 - 8 + 9 - 8 + 7 - 6 + 5 - 4\\&+ 3 - 2 + 1 - 2 + 3 - 4 = 40 - 40 = 0,\end{aligned}$$

so $r_{11} = 0$.

(d) The number is odd, so $r_2 = 1$.

(e) The number formed by the last two digits is $65 = 16 \times 4 + 1$, so $r_4 = 1$.

(f) The number formed by the last three digits is $765 = 95 \times 8 + 5$, so $r_8 = 5$.

(g) $r_6 \equiv 3r_2 - 2r_3 \equiv 3 - 4 \equiv -1 \equiv 5 \pmod 6$, so $r_6 = 5$.

(h) $r_{12} \equiv 4r_3 - 3r_4 \equiv 8 - 3 \equiv 5 \pmod{12}$, so $r_{12} = 5$.

(i) The required remainders are as follows.

4	321	234	567	898	765	
4	6	3	0	2	2	(mod 7)

Now

$$2 - 2 + 0 - 3 + 6 - 4 = 6 \pmod 7,$$

so $r_7 = 6$.

(j) The required remainders are as follows.

4	321	234	567	898	765	
4	9	0	8	1	11	(mod 13)

Now

$$11 - 1 + 8 - 0 + 9 - 4 \equiv 10 \pmod{13},$$

so $r_{13} = 10$.

(k) and (l) The remainders on division by 5 and 10 are the same as the remainders on division by 5 and 10 of the final digit, so $r_5 = 0$ and $r_{10} = 5$.

Solution 2.2

(a) If a has remainder r_3 on division by 3 and remainder r_5 on division by 5, then

$$a = 3q_3 + r_3 \quad \text{and} \quad a = 5q_5 + r_5,$$

where q_3 and q_5 are the respective quotients. Now

$$\begin{aligned}a &= 6a - 5a\\&= 6(5q_5 + r_5) - 5(3q_3 + r_3)\\&= 30q_5 - 15q_3 + 6r_5 - 5r_3\\&= 15(2q_5 - q_3) + 6r_5 - 5r_3.\end{aligned}$$

Thus $r_{15} \equiv 6r_5 - 5r_3 \pmod{15}$.

(b) In Exercise 2.1, we have $r_3 = 2$ and $r_5 = 0$, so $r_{15} \equiv -10 \pmod{15}$. Hence $r_{15} = 5$.

Solution 3.1

(a) 2 (b) 0 (c) 3 (d) 2

(e) 2 (f) 8 (g) 0

Solution 3.2

(a) A number in $\mathbb{Z}_{60}$ has a multiplicative inverse in $\mathbb{Z}_{60}$ if and only if it is coprime with 60.

(b) Any one of: 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59

(c) Any number in $0, 1, \ldots, 59$ that does not appear in the list in part (b).

Solution 3.3

(a) Using the Division Algorithm repeatedly:

$$\begin{aligned}7 &= 1 \times 5 + 2\\5 &= 2 \times 2 + 1.\end{aligned}$$

Eliminating multiples of 2:

$$\begin{aligned}1 &= 5 - 2 \times 2\\&= 5 - 2(7 - 1 \times 5)\\&= 5 - 2 \times 7 + 2 \times 5\\&= 3 \times 5 - 2 \times 7.\end{aligned}$$

Hence $3 \times 5 = 2 \times 7 + 1$, so the multiplicative inverse of 5 in $\mathbb{Z}_7$ is 3.

(b) Using the Division Algorithm repeatedly:

$$35 = 2 \times 12 + 11$$
$$12 = 1 \times 11 + 1.$$

Eliminating multiples of 11:

$$\begin{aligned} 1 &= 12 - 1 \times 11 \\ &= 12 - 1(35 - 2 \times 12) \\ &= 12 - 1 \times 35 + 2 \times 12 \\ &= 3 \times 12 - 1 \times 35 \end{aligned}$$

Hence $3 \times 12 = 1 \times 35 + 1$, so the multiplicative inverse of 12 in $\mathbb{Z}_{35}$ is 3.

(c) Using the Division Algorithm repeatedly:

$$\begin{aligned} 60 &= 2 \times 23 + 14 \\ 23 &= 1 \times 14 + 9 \\ 14 &= 1 \times 9 + 5 \\ 9 &= 1 \times 5 + 4 \\ 5 &= 1 \times 4 + 1. \end{aligned}$$

Eliminating multiples of 4, 5, 9 and 14:

$$\begin{aligned} 1 &= 5 - 1 \times 4 \\ &= 5 - (9 - 5) = 2 \times 5 - 9 \\ &= 2(14 - 9) - 9 = 2 \times 14 - 3 \times 9 \\ &= 2 \times 14 - 3(23 - 14) \\ &= 5 \times 14 - 3 \times 23 \\ &= 5(60 - 2 \times 23) - 3 \times 23 \\ &= 5 \times 60 - 13 \times 23 \end{aligned}$$

Hence $-13 \times 23 = -5 \times 60 + 1$ and, since $-13 \equiv 47 \pmod{60}$, the multiplicative inverse of 23 in $\mathbb{Z}_{60}$ is 47.

Solution 3.4

(a) Using Fermat's Little Theorem with $p = 11$ and noting that 7 is not a multiple of 11, we obtain

$$7^{10} \equiv 1 \pmod{11}.$$

Thus

$$7^{24} \equiv (7^{10})^2 \times 7^4 \equiv 1 \times 2401 \equiv 3 \pmod{11}.$$

Hence the remainder is 3.

(b) First note that

$$38 \equiv 4 \pmod{17} \quad \text{so} \quad 38^{51} \equiv 4^{51} \pmod{17}.$$

By Fermat's Little Theorem, $4^{16} \equiv 1 \pmod{17}$, so

$$4^{51} = (4^{16})^3 \times 4^3 \equiv 1 \times 64 \equiv 13 \pmod{17}.$$

Hence the remainder is 13.

(c) First note that

$$14 \equiv 4 \pmod 5 \quad \text{so} \quad 14^{200} \equiv 4^{200} \pmod 5.$$

By Fermat's Little Theorem, $4^4 \equiv 1 \pmod 5$, so

$$4^{200} \equiv (4^4)^{50} \equiv 1 \pmod 5.$$

Hence the remainder is 1.

Solution 4.1

(a) We have $26 = 5 \times 5 + 1$.

Rearranging gives $-5 \times 5 = -1 \times 26 + 1$.

Since $-5 \equiv 21 \pmod{26}$, the multiplicative inverse of 5 in $\mathbb{Z}_{26}$ is 21.

(b) The message is deciphered by applying $M_5^{-1}(c) = M_{21}(c) = 21 \times_{26} c$. We obtain

$$\begin{aligned} M_{21}(3) &= 21 \times_{26} 3 = 11, \\ M_{21}(25) &= 21 \times_{26} 25 = 5, \\ M_{21}(2) &= 21 \times_{26} 2 = 16, \\ M_{21}(17) &= 21 \times_{26} 17 = 19, \\ M_{21}(13) &= 21 \times_{26} 13 = 13, \\ M_{21}(19) &= 21 \times_{26} 19 = 9, \\ M_{21}(8) &= 21 \times_{26} 8 = 12, \\ M_{21}(18) &= 21 \times_{26} 18 = 14, \\ M_{21}(9) &= 21 \times_{26} 9 = 7. \end{aligned}$$

Hence the deciphered message is

$$\langle 11, 5, 5, 16, 19, 13, 9, 12, 9, 14, 7 \rangle,$$

which represents 'KEEP SMILING' in the English alphabet.

Solution 4.2

(a) Using the Division Algorithm repeatedly:

$$30 = 4 \times 7 + 2$$
$$7 = 3 \times 2 + 1.$$

Eliminating multiples of 2:

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3(30 - 4 \times 7) \\ &= 13 \times 7 - 3 \times 30 \end{aligned}$$

Thus $13 \times 7 = 3 \times 30 + 1$, so $13 \times 7 \equiv 1 \pmod{30}$ and hence the multiplicative inverse of 7 in $\mathbb{Z}_{30}$ is 13.

(b) To decipher the message, find $E_{13}(2)$ and $E_{13}(10)$. Repeated squaring gives

2^{2^n}	2^1	2^2	2^4	2^8
$2^{2^n} \pmod{31}$	2	4	16	8

so

$$\begin{aligned} 2^{13} &\equiv 2^1 \times 2^4 \times 2^8 \equiv 2 \times 16 \times 8 \pmod{31} \\ &= 256 \equiv 8 \pmod{31}. \end{aligned}$$

Thus $E_{13}(2) = 8$. Similarly, we have

10^{2^n}	10^1	10^2	10^4	10^8
10^{2^n} (mod 31)	10	7	18	14

so

$$10^{13} \equiv 10^1 \times 10^4 \times 10^8 \equiv 10 \times 18 \times 14 \pmod{31}$$
$$\equiv 2520 \equiv 9 \pmod{31}.$$

Thus $E_{13}(10) = 9$.

Hence the deciphered message is $\langle 8, 9\rangle$, which represents 'HI' in the English alphabet.

Solution 4.3

Note that $51 = 3 \times 17$, so with $p = 3$ and $q = 17$ we obtain $(p-1)(q-1) = 32$. Thus, to find the inverse function for the RSA cipher R_{25} on $\mathbb{Z}_{51}$, we need to determine the multiplicative inverse of 25 in $\mathbb{Z}_{32}$.

(a) Using the Division Algorithm repeatedly:

$$32 = 1 \times 25 + 7$$
$$25 = 3 \times 7 + 4$$
$$7 = 1 \times 4 + 3$$
$$4 = 1 \times 3 + 1.$$

Eliminating multiples of 3, 4 and 7:

$$\begin{aligned} 1 &= 4 - 1 \times 3 \\ &= 4 - 1(7 - 1 \times 4) \\ &= 2 \times 4 - 1 \times 7 \\ &= 2(25 - 3 \times 7) - 1 \times 7 \\ &= 2 \times 25 - 7 \times 7 \\ &= 2 \times 25 - 7(32 - 1 \times 25) \\ &= 9 \times 25 - 7 \times 32 \end{aligned}$$

So $9 \times 25 = 7 \times 32 + 1$ and the multiplicative inverse of 25 in $\mathbb{Z}_{32}$ is 9.

(b) From part (a) we have $R_{25}^{-1} = R_9$. Thus we need to find

$$R_9(8), R_9(29), R_9(39), R_9(16).$$

In each case we use repeated squaring.

8^{2^n}	8^1	8^2	8^4	8^8
8^{2^n} (mod 51)	8	13	16	1

Thus

$$8^9 \equiv 8^8 \times 8^1 \equiv 1 \times 8 \equiv 8 \pmod{51},$$

so $R_9(8) = 8$.

29^{2^n}	29^1	29^2	29^4	29^8
29^{2^n} (mod 51)	29	25	13	16

Thus

$$29^9 \equiv 29^8 \times 29^1 \equiv 16 \times 29 \equiv 5 \pmod{51},$$

so $R_9(29) = 5$.

39^{2^n}	39^1	39^2	39^4	39^8
39^{2^n} (mod 51)	39	42	30	33

Thus

$$39^9 \equiv 39^8 \times 39^1 \equiv 33 \times 39 \equiv 12 \pmod{51},$$

so $R_9(39) = 12$.

16^{2^n}	16^1	16^2	16^4	16^8
16^{2^n} (mod 51)	16	1	1	1

Thus

$$16^9 \equiv 16^8 \times 16^1 \equiv 1 \times 16 \equiv 16 \pmod{51},$$

so $R_9(16) = 16$.

Hence the deciphered message is $\langle 8, 5, 12, 16\rangle$, which represents 'HELP' in the English alphabet

Solutions for Chapter D3

Solution 1.1

(a) Here r_π is rotation about O through π, and

$$r_\pi(1,0) = (-1,0).$$

(b) Here q_0 is reflection in the x-axis, and

$$q_0(2,0) = (2,0)$$

(c) Here $q_{\pi/4}$ is a reflection in the line $y = x$, and

$$q_{\pi/4}(1,2) = (2,1).$$

(d) Here $r_{3\pi/2}$ is rotation about O through $3\pi/2$, and

$$r_{3\pi/2}(2,3) = (3,-2).$$

Solution 1.2

$$S(\text{OCT}) = \{e, r_{\pi/4}, r_{\pi/2}, r_{3\pi/4}, r_\pi, r_{5\pi/4}, r_{3\pi/2}, r_{7\pi/4},$$
[illegible] $\}$

Solution 1.3

(a) We have

$$r_{\pi/3} \circ r_{5\pi/3} = r_{2\pi \,(\mathrm{mod}\, 2\pi)} = r_0 = e.$$

(b) We have

$$q_{\pi/2} \circ q_{\pi/4} = r_{\pi - \pi/2 \,(\mathrm{mod}\, 2\pi)} = r_{\pi/2}.$$

(c) We have

$$r_\pi \circ q_{\pi/2} = q_{\pi/2 + \pi/2 \,(\mathrm{mod}\, \pi)} = q_0.$$

Solution 1.4

Hint: You can save time by finding the easy entries first, such as $q_\phi \circ q_\phi = e$, and then looking for patterns.

$\circ$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$
e	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$
$r_{\pi/3}$	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$	q_0
$r_{2\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$	q_0	$q_{\pi/6}$
r_π	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$
$r_{4\pi/3}$	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$q_{2\pi/3}$	$q_{5\pi/6}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$
$r_{5\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$q_{5\pi/6}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$
q_0	q_0	$q_{5\pi/6}$	$q_{2\pi/3}$	$q_{\pi/2}$	$q_{\pi/3}$	$q_{\pi/6}$	e	$r_{5\pi/3}$	$r_{4\pi/3}$	r_π	$r_{2\pi/3}$	$r_{\pi/3}$
$q_{\pi/6}$	$q_{\pi/6}$	q_0	$q_{5\pi/6}$	$q_{2\pi/3}$	$q_{\pi/2}$	$q_{\pi/3}$	$r_{\pi/3}$	e	$r_{5\pi/3}$	$r_{4\pi/3}$	r_π	$r_{2\pi/3}$
$q_{\pi/3}$	$q_{\pi/3}$	$q_{\pi/6}$	q_0	$q_{5\pi/6}$	$q_{2\pi/3}$	$q_{\pi/2}$	$r_{2\pi/3}$	$r_{\pi/3}$	e	$r_{5\pi/3}$	$r_{4\pi/3}$	r_π
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/3}$	$q_{\pi/6}$	q_0	$q_{5\pi/6}$	$q_{2\pi/3}$	r_π	$r_{2\pi/3}$	$r_{\pi/3}$	e	$r_{5\pi/3}$	$r_{4\pi/3}$
$q_{2\pi/3}$	$q_{2\pi/3}$	$q_{\pi/2}$	$q_{\pi/3}$	$q_{\pi/6}$	q_0	$q_{5\pi/6}$	$r_{4\pi/3}$	r_π	$r_{2\pi/3}$	$r_{\pi/3}$	e	$r_{5\pi/3}$
$q_{5\pi/6}$	$q_{5\pi/6}$	$q_{2\pi/3}$	$q_{\pi/2}$	$q_{\pi/3}$	$q_{\pi/6}$	q_0	$r_{5\pi/3}$	$r_{4\pi/3}$	r_π	$r_{2\pi/3}$	$r_{\pi/3}$	e

Solution 2.1

A pair of inverse elements can be found in the table borders above and to the left of each e in the table.

Element	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$
Inverse	e	$r_{5\pi/3}$	$r_{4\pi/3}$	r_π	$r_{2\pi/3}$	$r_{\pi/3}$	q_0	$q_{\pi/6}$	$q_{\pi/3}$	$q_{\pi/2}$	$q_{2\pi/3}$	$q_{5\pi/6}$

Solution 2.2

Using the Cayley table, we obtain

$$q_{\pi/3} \circ (r_{2\pi/3} \circ q_{5\pi/6}) = q_{\pi/3} \circ q_{\pi/6} = r_{\pi/3}$$

and

$$(q_{\pi/3} \circ r_{2\pi/3}) \circ q_{5\pi/6} = q_0 \circ q_{5\pi/6} = r_{\pi/3}.$$

This verifies that the associative property holds in this particular case.

Solution 2.3

(a) The number 0 is in $\mathbb{Q}$, but 0 does not have a multiplicative inverse: there is no rational number p such that $p \times 0 = 0 \times p = 1$. Since axiom G3 does not hold, $(\mathbb{Q}, \times)$ is not a group.

(b) $(\mathbb{Q}^*, \times)$ is a group, as it does satisfy all four axioms. The verification of the axioms is similar to that for $(\mathbb{R}^*, \times)$ in Activity 2.3.

Solution 2.4

(a) Let $G = \{1, 3, 5, 7\}$. Since G is finite, a Cayley table can be formed.

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

All the elements in the body of the table are in G, so axiom G1 holds.

The element 1 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold.

Also axiom G4 holds, since $\times_8$ is associative on $\mathbb{Z}_8$ and hence on G. Hence $(G, \times_8)$ is a group.

Since the Cayley table is symmetric about the main diagonal, the group is Abelian.

(b) Let $G = \{1, 3, 7, 9\}$. Since G is finite, a Cayley table can be formed.

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

All the elements in the body of the table are in G, so axiom G1 holds.

The element 1 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold.

Also axiom G4 holds, since $\times_{10}$ is associative on $\mathbb{Z}_{10}$ and hence on G. Hence $(G, \times_{10})$ is a group.

Since the Cayley table is symmetric about the main diagonal, the group is Abelian.

(c) Let $G = \{1, 5, 7, 11\}$. Since G is finite, a Cayley table can be formed.

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

All the elements in the body of the table are in G, so axiom G1 holds.

The element 1 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold.

Also axiom G4 holds, since $\times_{12}$ is associative on $\mathbb{Z}_{12}$ and hence on G. Hence $(G, \times_{12})$ is a group.

Since the Cayley table is symmetric about the main diagonal, the group is Abelian.

(d) Let $G = \{2, 4\}$. Since G is finite, a Cayley table can be formed.

$\times_6$	2	4
2	4	2
4	2	4

All the elements in the body of the table are in G, so axiom G1 holds.

The element 4 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold.

Also axiom G4 holds, since $\times_6$ is associative on $\mathbb{Z}_6$ and hence on G. Hence $(G, \times_6)$ is a group.

Since the Cayley table is symmetric about the main diagonal, the group is Abelian.

(e) Let $G = \{0, 2, 4, 6, 8\}$. Since G is finite, a Cayley table can be formed.

[illegible]	0	2	[illegible]	[illegible]	8
[illegible]	[illegible]	2	[illegible]	[illegible]	8
2	[illegible]	4	6	8	[illegible]
4	[illegible]	6	8	[illegible]	2
6	6	8	0	2	4
8	8	0	2	4	6

All the elements in the body of the table are in G, so axiom G1 holds.

The element 0 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold.

Also axiom G4 holds, since $+_{10}$ is associative on $\mathbb{Z}_{10}$ and hence on G. Hence $(G, +_{10})$ is a group.

Since the Cayley table is symmetric about the main diagonal, the group is Abelian.

Solution 2.5

(a) The Cayley table is

$\times$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

All the entries in the table are in the set $M = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$, so axiom G1 holds.

The element $\mathbf{I}$ acts as the identity and it appears symmetrically in each row and column, so axioms G2 and G3 hold.

Matrix multiplication is associative, so axiom G4 holds.

Hence M is a group under matrix multiplication.

(b) The matrices $\mathbf{I}$, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ represent the symmetries e, $q_{\pi/2}$, r_π, q_0, respectively, and the set $\{e, r_\pi, q_0, q_{\pi/2}\}$ together with the operation of composition of functions is $(S(\square), \circ)$, the symmetry group of the rectangle. So $(M, \times)$ corresponds to $(S(\square), \circ)$.

Solution 2.6

Let $G = \{3k : k \in \mathbb{Z}\}$.

Closure

Consider any two elements of G, say $3k$ and $3m$, where $k, m \in \mathbb{Z}$. Then

$$3k + 3m = 3(k + m) \in G,$$

since $k + m \in \mathbb{Z}$, so G is closed under $+$.

Identity

Since $0 = 3 \times 0$ and $0 \in \mathbb{Z}$, we have $0 \in G$, and

$$3k + 0 = 3k = 0 + 3k,$$

for all $k \in \mathbb{Z}$, so 0 is an identity element.

Inverses

Consider any element of G, say $3k$, where $k \in \mathbb{Z}$.

Then $-3k = 3(-k)$ is in G, since $-k \in \mathbb{Z}$, and

$$3k + (-3k) = 0 = (-3k) + 3k,$$

so each element of G has an inverse.

Associativity

This holds since $+$ is associative on $\mathbb{Z}$.

Hence $(G, +)$ forms a group.

Solution 2.7

Let $G = \{5^k : k \in \mathbb{Z}\}$.

Closure

Consider any two elements of G, say 5^k and 5^m, where $k, m \in \mathbb{Z}$. Then

$$5^k \times 5^m = 5^{k+m} \in G,$$

since $k + m \in \mathbb{Z}$, so G is closed under $\times$.

Identity

Since $1 = 5^0$ and $0 \in \mathbb{Z}$, we have $1 \in G$, and

$$5^k \times 1 = 5^k = 1 \times 5^k,$$

for all $k \in \mathbb{Z}$, so 1 is an identity element.

Inverses

Consider any element of G, say 5^k, where $k \in \mathbb{Z}$.

Then $5^{(-k)}$ is in G, since $-k \in \mathbb{Z}$, and

[illegible]

so each element of G has an inverse.

Associativity

This holds since $\times$ is associative on $\mathbb{Z}$.

Hence $(G, \times)$ forms a group.

Solution 2.8

(a) The identity element is e. Consider the entry for $x * y$. This cannot be y, because x is not the identity, and it cannot be x, because y is not the identity. So, $x * y = e$. The other entries can be filled in using the property that no element can be repeated in any row or column. The completed table is as follows.

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

(b) Since no element can be repeated in any row or column, the missing element in column w must be y, and in row z the missing element must be z. Using the same rule, column z and row x can now be completed.

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Now, the entry corresponding to $y * y$ cannot be x or y or w, for the same reason. So it must be z and the table can now be completed.

$*$	w	x	y	z
w	z	y	x	w
x	y	z	w	x
y	x	w	z	y
z	w	x	y	[illegible]

Solution 2.9

We have

$$(g * h * g^{-1})^n = (g * h * g^{-1}) * (g * h * g^{-1}) * \cdots * (g * h * g^{-1}),$$

with n brackets,

$$= g * h * (g^{-1} * g) * h * (g^{-1} * g) * \cdots * (g^{-1} * g) * h * g^{-1},$$

with n h's,

$$= g * h * e * h * e * \cdots * e * h * g^{-1}$$

$$= g * h^n * g^{-1}, \quad \text{since } e * h = h = h * e.$$

Solution 3.1

The Cayley tables for $(\mathbb{Z}_4, +_4)$ and $(\{e, r_{\pi/2}, r_\pi, r_{3\pi/2}\}, \circ)$, the subgroup of $(S(\square), \circ)$ consisting of rotations of a square, are shown below:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\circ$	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$
e	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$
$r_{\pi/2}$	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	e
r_π	r_π	$r_{3\pi/2}$	e	$r_{\pi/2}$
$r_{3\pi/2}$	$r_{3\pi/2}$	e	$r_{\pi/2}$	r_π

The patterns in the tables indicate that these groups are isomorphic to each other, a suitable isomorphism ϕ being

$$\phi(0) = e, \ \phi(1) = r_{\pi/2}, \ \phi(2) = r_\pi, \ \phi(3) = r_{3\pi/2}.$$

Any plane set with these three non-trivial rotational symmetries and no reflectional symmetry will have this symmetry group. One example is shown below.

Solution 3.2

(a) The following arrangement gives the required pattern

$*$	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

(b) An isomorphism ϕ from $(S(\square), \circ)$ to the group in Exercise 2.8(b) is

$$\phi(e) = z, \ \phi(r_\pi) = w, \ \phi(q_0) = x, \ \phi(q_{\pi/2}) = y.$$

Solution 3.3

The required group is in part (b) of Exercise 2.4. Rearranging the Cayley table in part (b), we obtain the following

[illegible]	[illegible]	3	9	7
[illegible]	[illegible]	3	9	7
3	3	9	[illegible]	1
9	9	7	1	3
7	7	1	3	9

Now the pattern in the Cayley table above is the same as the pattern in the Cayley table for the rotations of the square, shown in Solution 3.1. A specific isomorphism ϕ is given by

$$\phi(e) = 1, \ \phi(r_{\pi/2}) = 3, \ \phi(r_\pi) = 9, \ \phi(r_{3\pi/2}) = 7.$$

(The groups in parts (a) and (c) have a different number of self-inverse elements, whereas the groups in parts (d) and (e) have a different number of elements.)

Solution 3.4

(a) The row and column for x reproduce the order of the elements on the borders, so x is the identity element.

(b)

Element	a	b	c	d	e	x	y	z
Inverse	e	z	d	c	a	x	y	b

(c) The group has 8 elements and is not Abelian, since it is not symmetric about the main diagonal of the Cayley table. The only two possibilities are therefore $(S(\square), \circ)$ and $(QUAT, \times)$. Since the identity element x appears twice in the main diagonal, two elements of the group are self-inverse. The only possibility is then $(QUAT, \times)$.

Solution 3.5

The group $(\mathbb{Z}_6, +_6)$ has two self-inverse elements: 0 and 3.

The group $(S(\Delta), \circ)$ has four self-inverse elements:

[illegible]

Since they have different numbers of self-inverse elements, the two groups cannot be isomorphic to each other.

Solutions for Chapter D4

Solution 1.1

(a) This statement is true. Since

$$x^2 - 2x - 15 = (x + 3)(x - 5),$$

the equation $x^2 - 2x = 15$ is true when $x = -3$ and $x = 5$

(b) This statement is true. Let a and b be real numbers with $a > b$. Then

$$\begin{aligned} f(a) - f(b) &= 3a + 2 - (3b + 2) \\ &= 3a - 3b \\ &= 3(a - b) > 0, \end{aligned}$$

since $a > b$.

Since $a > b \Rightarrow f(a) > f(b)$, for all real a, b, the function is increasing on its domain $\mathbb{R}$

(c) This statement is false. A counter-example is

$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & \cdot \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ [illegible]

(d) This statement is true. If 2 divides n, then $n = 2m$, for some integer m. Hence

$$n^2 = (2m)^2 = 4m^2$$

and, as m^2 is an integer, we deduce that 4 divides n^2.

(e) The result looks plausible at first, as the following examples show.

n	$n^2 + n + 41$	n	$n^2 + n + 41$
1	43	6	83
2	47	7	97
3	53	8	113
4	61	9	131
5	71	10	151

However, in general it is false. A counter-example is $n = 41$:

$$41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \times 43,$$

which is not prime.

Solution 1.2

The problem here is multiplying the first inequality by a negative number. Since $\ln(0.5) < 0$ and $2 > 1$, we should obtain

$$2\ln(0.5) < \ln(0.5).$$

Solution 1.3

Since $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, there are only five cases to consider:

$$\begin{aligned} 0^3 &\equiv 0 \pmod 5, \\ 1^3 &\equiv 1 \pmod 5, \\ 2^3 &\equiv 3 \pmod 5, \\ 3^3 &\equiv 2 \pmod 5, \\ 4^3 &\equiv 4 \pmod 5. \end{aligned}$$

So $x = 4$ is the only solution of $x^3 = 4$ in $\mathbb{Z}_5$.

Solution 1.4

If 3 divides n, then $n \equiv 0 \pmod 3$, so

$$5n - 6 \equiv 0 - 6 \equiv 0 \pmod 3,$$

using properties of congruences from Chapter D2. Thus if 3 divides n, then 3 divides $5n - 6$.

Alternatively, we can write $n = 3k$, where $k \in \mathbb{Z}$, so

$$5n - 6 = 5 \times 3k - 6 = 3(5k - 2).$$

Thus $5n - 6$ is divisible by 3, since $5k - 2 \in \mathbb{Z}$.

Solution 1.5

The product of three consecutive positive integers can be written as $n(n + 1)(n + 2)$, where $n \in \mathbb{N}$.

At least one of n, $n + 1$, $n + 2$ is divisible by 2 and at least one is divisible by 3; see Exercise 1.1(c), Chapter D4. Since the product is divisible by 2 and by 3, it is divisible by 6.

Solution 1.6

There are two cases to consider:

(i) n has remainder 1 on division by 3; that is, $n \equiv 1 \pmod 3$. In this case, $n^2 \equiv 1 \times 1 \equiv 1 \pmod 3$, so n^2 has remainder 1 upon division by 3.

(ii) n has remainder 2 on division by 3, that is, $n \equiv 2 \pmod 3$. In this case, $n^2 \equiv 2 \times 2 \equiv 4 \equiv 1 \pmod 3$, so n^2 again has remainder 1 upon division by 3.

So if n is not divisible by 3, then n^2 has remainder 1 on division by 3.

Solution 1.7

For real numbers a and b, if $f(a) = f(b)$, then

$$4a + 5 = 4b + 5 \quad \text{so} \quad a = b.$$

Since $f(a) = f(b) \Rightarrow a = b$, the function f is indeed one-one.

Solution 1.8

Let $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ be elements of S, so $ab = cd = 1$. Then

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}.$$

This is of the correct form to be an element of S, provided that $ac \times bd = 1$. But

$$\begin{aligned} ac \times bd &= ab \times cd, \\ &= 1 \times 1, \text{ by assumption,} \\ &= 1, \end{aligned}$$

as required. So S is closed under matrix multiplication.

Solution 1.9

Let $n = 2u$ and $m = 2v$ represent even integers and let $a = 2k + 1$ and $b = 2l + 1$ represent odd integers; here we have $u, v, k, l \in \mathbb{Z}$.

(a) (i) We have

$$a + b = 2k + 1 + 2l + 1 = 2(k + l + 1) = 2p,$$

where $p \in \mathbb{Z}$. So the sum of any two odd integers is even.

(ii) We have

$$n + m = 2u + 2v = 2(u + v) = 2q,$$

where $q \in \mathbb{Z}$. So the sum of any two even integers is even.

(iii) We have

$$n + a = 2u + 2k + 1 = 2(u + k) + 1 = 2r + 1,$$

where $r \in \mathbb{Z}$. So the sum of an odd integer and an even integer is odd.

(b) (i) We have

$$\begin{aligned} a^2 &= (2k + 1)^2 = 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 = 2s + 1, \end{aligned}$$

where $s \in \mathbb{Z}$. So the square of an odd integer is odd.

(ii) We have

$$n^2 = (2u)^2 = 4u^2 = 2(2u^2) = 2t,$$

where $t \in \mathbb{Z}$. So the square of an even integer is even.

Solution 1.10

Assume that n^2 is divisible by 3, but that n is not divisible by 3. Since n is not divisible by 3, we deduce by the result of Exercise 1.6 that n^2 has remainder 1 on division by 3.

The assumption that n is not divisible by 3 has led to a contradiction with the assumption that n^2 is divisible by 3. Therefore if n^2 is divisible by 3, then n is also divisible by 3.

Solution 2.1

(a) $a(n)$ is necessary but not sufficient.

$b(n)$ is necessary but not sufficient.

$c(n)$ is necessary but not sufficient.

$d(n)$ is sufficient but not necessary.

(b) A necessary and sufficient condition for n to be divisible by 10 is $a(n) \wedge c(n)$.

(c) If n is divisible by 2 and n is divisible by 5, then n is divisible by 40.

(d) The converse of the proposition in part (c) is:

$$d(n) \Rightarrow (a(n) \wedge c(n));$$

that is, if n is divisible by 40, then it is divisible by both 2 and 5.

(e) A counter-example is $n = 10$.

Solution 2.2

(a) The converse proposition is:

if $\sin\theta = 0$, then $\theta = \pi$.

(b) The original proposition is true, by direct calculation.

(c) The converse proposition is not true. A counter-example is $\theta = 4\pi$.

Solution 2.3

(a) This is a valid deduction. Rewrite the first premise as

if it is hot day, then my plants must be watered.

Define propositions p and q as follows:

p means: it is a hot day;
q means: my plants must be watered.

Then the propositions known to be true are p and $p \Rightarrow q$, and the conclusion is that proposition q is true. So, this argument is of the form Modus Ponens.

(b) This is not a valid deduction. Rewrite the first premise as

if it is Saturday, then Greg goes to the mountains.

Define propositions p and q as follows:

p means: it is Saturday;
q means: Greg goes to the mountains.

The propositions known to be true are q and $p \Rightarrow q$. The argument attempts to deduce that p is true. This is not a valid argument. (Greg might go to the mountains on a Sunday also.)

(c) This argument is valid. It is not of the form Modus Ponens, though. It can be related to Modus Ponens, but it needs to be combined with the use of proof by contradiction. Rewrite the first premise as

if x is an elephant, then x has a trunk,

where x is in, say, the set of all animals.

Applying this proposition to the particular case where x is Zeya gives

if Zeya is an elephant, then Zeya has a trunk.

Define the propositions p and q to be:

p means: Zeya is an elephant;
q means: Zeya has a trunk.

Then, the proposition $p \Rightarrow q$ is true. Now, *assume* that Zeya is an elephant; that is, that p is true. Then it can be deduced by Modus Ponens that Zeya has a trunk. However, this contradicts the second premise. So the assumption that Zeya is an elephant must be false. Thus, it can be concluded that Zeya is not an elephant.

(d) Define propositions p and q as follows:

p means: $(H, *)$ and $(G, \diamond)$ are finite isomorphic groups;
q means: $|G| = |H|$.

Then it is given that the proposition $p \Rightarrow q$ is true and that p is false. The claim is that q is false. This is not a valid deduction. (For example, $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$ are finite non-isomorphic groups with $|(\mathbb{Z}_4, +_4)| = |(S(\square), \circ)|$.)

Solution 3.1

Let $p(n)$ be the variable proposition

$$x^n \equiv y^n (\text{mod } m).$$

First we check that $p(1)$ is true.

Since it is given that $x \equiv y \pmod{m}$, we deduce that $p(1)$ is true immediately.

Next we assume that $p(k)$ is true, that is, $x^k \equiv y^k \pmod{m}$, and we try to deduce that $p(k+1)$ is true, that is, $x^{k+1} \equiv y^{k+1} \pmod{m}$.

Since $x^k \equiv y^k \pmod{m}$, we have

$$x \times x^k \equiv y \times y^k \pmod{m},$$

by Chapter D2, Theorem 1.2(e).

Thus

$$x^{k+1} \equiv y^{k+1} \pmod{m},$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.2

(a) $$\mathbf{A}^2 = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix},$$

$$\mathbf{A}^3 = \begin{pmatrix} 1 & 7 \\ 0 & 8 \end{pmatrix},$$

$$\mathbf{A}^4 = \begin{pmatrix} 1 & 15 \\ 0 & 16 \end{pmatrix},$$

$$\mathbf{A}^5 = \begin{pmatrix} 1 & 31 \\ 0 & 32 \end{pmatrix}.$$

A plausible conjecture is that

$$\mathbf{A}^n = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}, \text{ for } n = 1, 2, \ldots .$$

(b) Let $p(n)$ be the variable proposition

$$\mathbf{A}^n = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}.$$

For $n = 1$, we have $\mathbf{A}^1 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ and

$$\begin{pmatrix} 1 & 2^1 - 1 \\ 0 & 2^1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

So $p(1)$ is true.

Next we assume that $p(k)$ is true, that is,

$$\mathbf{A}^k = \begin{pmatrix} 1 & 2^k - 1 \\ 0 & 2^k \end{pmatrix},$$

and we try to deduce that $p(k+1)$ is true, that is,

$$\mathbf{A}^{k+1} = \begin{pmatrix} 1 & 2^{k+1} - 1 \\ 0 & 2^{k+1} \end{pmatrix}.$$

Now, since $p(k)$ is true, we have

$$\begin{aligned}\mathbf{A}^{k+1} &= \mathbf{A}^k \times \mathbf{A} \\ &= \begin{pmatrix} 1 & 2^k - 1 \\ 0 & 2^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 + 2(2^k - 1) \\ 0 & 2^k \times 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2^{k+1} - 1 \\ 0 & 2^{k+1} \end{pmatrix},\end{aligned}$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.3

Let $p(n)$ be the variable proposition

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}.$$

For $n = 1$, the left-hand side gives

$$1 \times 2 \times 3 = 6,$$

and the right-hand side gives

$$\frac{n(n+1)(n+2)(n+3)}{4} = \frac{1 \times 2 \times 3 \times 4}{4} = 6.$$

So $p(1)$ is true.

Next we assume that $p(k)$ is true, that is,

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + k(k+1)(k+2) = \frac{k(k+1)(k+2)(k+3)}{4},$$

and we try to deduce that $p(k+1)$ is true, that is,

$$1 \times 2 \times 3 + \cdots + (k+1)(k+2)(k+3) = \frac{(k+1)(k+2)(k+3)(k+4)}{4}.$$

Now

$$\begin{aligned}&1 \times 2 \times 3 + \cdots + k(k+1)(k+2) + (k+1)(k+2)(k+3) \\ &\quad = \frac{k(k+1)(k+2)(k+3)}{4} + (k+1)(k+2)(k+3), \\ &\qquad\qquad \text{since } p(k) \text{ is true,} \\ &\quad = (k+1)(k+2)(k+3)\left(\frac{k}{4} + 1\right) \\ &\quad = \frac{(k+1)(k+2)(k+3)(k+4)}{4},\end{aligned}$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.4

Let $p(n)$ be the variable proposition $u_n > 3$.

Now $u_1 = 3.5 > 3$, so $p(1)$ is true.

Next we assume that $p(k)$ is true, that is, $u_k > 3$, and we try to deduce that $p(k+1)$ is true, that is, $u_{k+1} > 3$.

Since $u_k > 3$, we have $u_k + 2 > 5$, so

$$\frac{5}{u_k + 2} < \frac{5}{5} = 1,$$

and hence

$$u_{k+1} = 4 - \frac{5}{u_k + 2} > 4 - 1 = 3,$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.5

Let $p(n)$ be the variable proposition

$$\sum_{r=1}^{n} \frac{r}{2^r} = 2 - \frac{n+2}{2^n}.$$

For $n = 1$, the sum is

$$\frac{1}{2^1} = \frac{1}{2},$$

and the right-hand side gives

$$2 - \frac{1+2}{2^1} = 2 - \frac{3}{2} = \frac{1}{2}.$$

So $p(1)$ is true.

Next we assume that $p(k)$ is true, that is,

$$\sum_{r=1}^{k} \frac{r}{2^r} = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{k}{2^k} = 2 - \frac{k+2}{2^k},$$

and we try to deduce that $p(k+1)$ is true, that is,

$$\sum_{r=1}^{k+1} \frac{r}{2^r} = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{k}{2^k} + \frac{k+1}{2^{k+1}}$$
$$= 2 - \frac{(k+1)+2}{2^{k+1}}.$$

Now

$$\begin{aligned}\sum_{r=1}^{k+1} \frac{r}{2^r} &= \frac{1}{2} + \frac{2}{2^2} + \frac{3}{3^3} + \cdots + \frac{k}{2^k} + \frac{k+1}{2^{k+1}}\\ &= 2 - \frac{k+2}{2^k} + \frac{k+1}{2^{k+1}}, \text{ since } p(k) \text{ is true,}\\ &= 2 - \frac{2(k+2)}{2^{k+1}} + \frac{k+1}{2^{k+1}}\\ &= 2 - \frac{2k+4}{2^{k+1}} + \frac{k+1}{2^{k+1}}\\ &= 2 - \frac{k+3}{2^{k+1}} = 2 - \frac{(k+1)+2}{2^{k+1}},\end{aligned}$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.6

Let $p(n)$ be the variable proposition

$$f^{(n)}(x) = x^2e^x + 2nxe^x + n(n-1)e^x,$$

where $f(x) = x^2e^x$. First we check that $p(1)$ is true. Using the product rule, we have

$$f'(x) = x^2e^x + 2xe^x.$$

Substituting $n = 1$ into the formula for $f^{(n)}(x)$ proposed above gives

$$x^2e^x + 2xe^x + 1(1-1)e^x = x^2e^x + 2xe^x.$$

So $p(1)$ is true.

Next we assume that $p(k)$ is true, that is,

$$f^{(k)}(x) = x^2e^x + 2kxe^x + k(k-1)e^x,$$

and we try to deduce that $p(k+1)$ is true, that is,

$$f^{(k+1)}(x) = x^2e^x + 2(k+1)xe^x + (k+1)ke^x.$$

Now $f^{(k+1)}(x)$ is just the derivative of $f^{(k)}(x)$ so, since $p(k)$ is true,

$$\begin{aligned}f^{(k+1)}(x) &= \frac{d}{dx}\left(x^2e^x + 2kxe^x + k(k-1)e^x\right)\\ &= (x^2e^x + 2xe^x) + (2kxe^x + 2ke^x)\\ &\quad + k(k-1)e^x, \text{ using the product rule,}\\ &= x^2e^x + (2+2k)xe^x + (2k + k(k-1))\, e^x\\ &= x^2e^x + 2(k+1)xe^x + (k+1)ke^x,\end{aligned}$$

as required.

Since $p(1)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \in \mathbb{N}$, we deduce that $p(n)$ is true for all $n \in \mathbb{N}$, by mathematical induction.

Solution 3.7

Let $p(n)$ be the variable proposition

$$n! > 2^n.$$

For $n = 4$, we have

$$n! = 4! = 24 \quad \text{and} \quad 2^n = 2^4 = 16,$$

so $p(4)$ is true.

Next we assume that $p(k)$ is true, that is,

$$k! > 2^k,$$

and try to deduce that $p(k+1)$ is true, that is,

$$(k+1)! > 2^{k+1},$$

or equivalently

$$(k+1)! - 2^{k+1} > 0.$$

But

$$\begin{aligned}(k+1)! - 2^{k+1} &= (k+1)k! - 2 \times 2^k\\ &> (k+1)2^k - 2 \times 2^k,\\ &\quad \text{since } k! > 2^k,\\ &= (k-1)2^k\\ &> 0, \text{ since } k > 1,\end{aligned}$$

as required.

Since $p(4)$ is true, and if $p(k)$ is true, then $p(k+1)$ is true, for $k \geq 4$, we deduce that $p(n)$ is true for all $n \geq 4$, by mathematical induction.

Printed in the United Kingdom by Lithmark Limited, Hitchin.